CTIC
Center for Technology, Innovation and Competition

Penn Law

Overcoming Legal Barriers to RPKI Adoption

Christopher S. Yoo
University of Pennsylvania

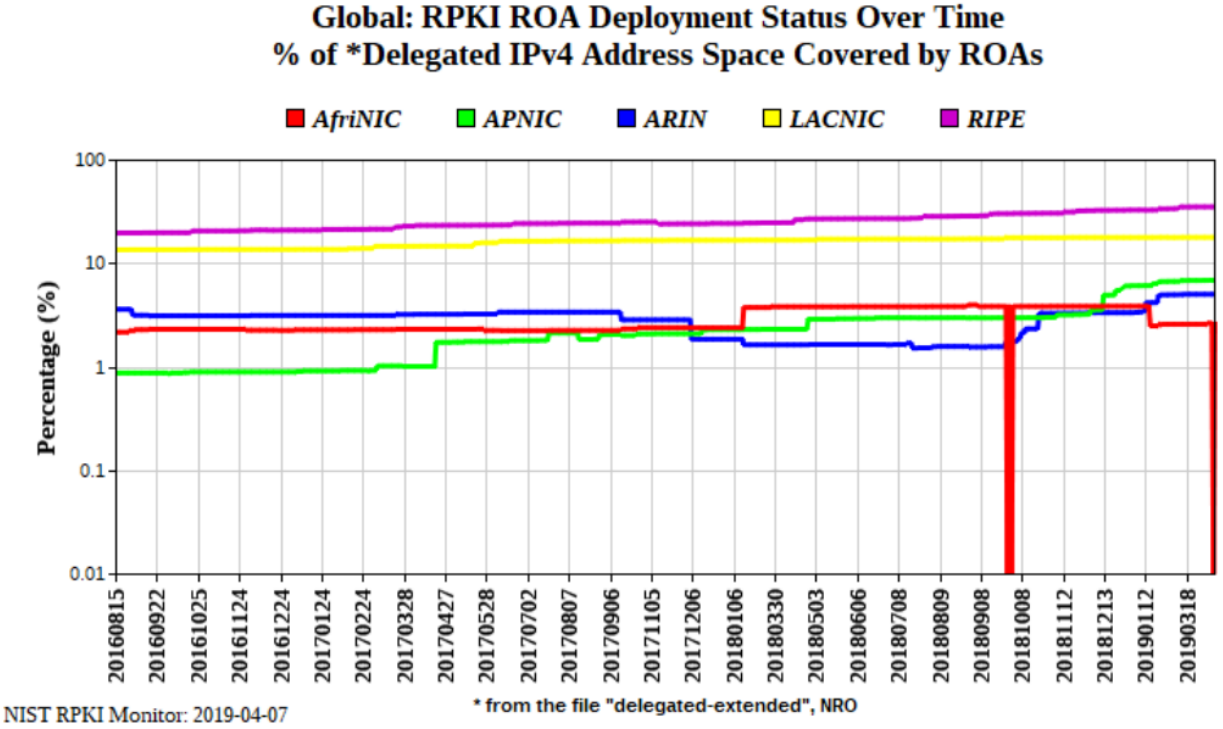
April 9, 2019

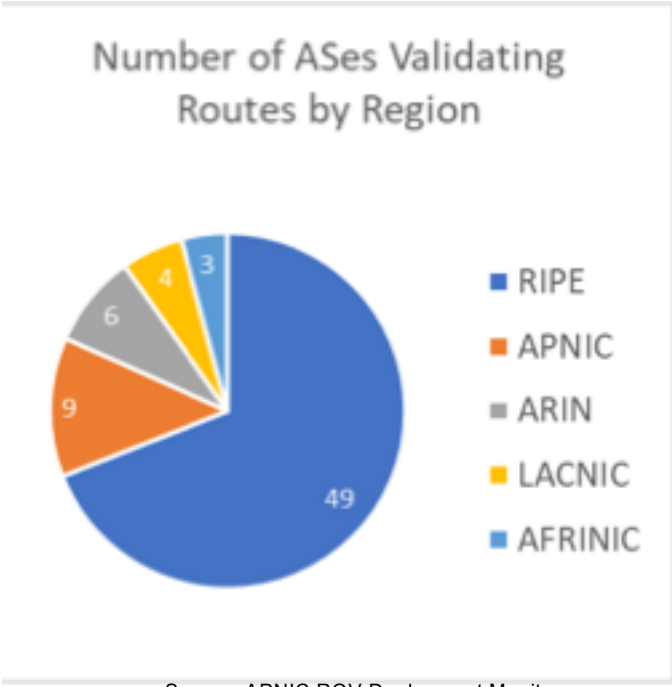
Research supported by NSF EAGER Award #1748362

Intro to Resource Public Key Infrastructure (RPKI)

- RPKI protects against route highjacks by authenticating route origins
  - IP address holders create certificates identifying authentic IP address origins
  - ISPs use validator software to verify that routes are pointing to correct origins
- Last 12 months have been eventful for RPKI
  - Highjacks of Cloudflare DNS in May 2018 and Amazon DNS in Aug. 2018
  - NTT began combining RPKI information with IRR data in July 2018
  - Cloudflare committed to RPKI and began developing own validator software
  - AT&T began filtering (dropping invalids) routes in Feb. 2019
  - Google has begun flagging routes and will begin filtering routes in 2019
  - 100+ networks joined ISOC's Mutually Agreed Norms for Routing Security

Global RPKI Deployment





Source: APNIC ROV Deployment Monitor

- 80% of those engaging in ROV omit the ARIN TAL (Cartwright-Cox, 2018)

NSF Grant on Legal Barriers to RPKI Adoption

- Motivation: reports that legal issues were slowing RPKI adoption in the ARIN region (particularly the RPA's indemnification clause)
- Methodology
  - Analysis of relevant contracts and policies
  - Interviews with broad range of stakeholders
  - Engagement with the ARIN and NANOG communities
- Milestones
  - Presentations at NANOG 73 (June 2018), 74 (Oct. 2018), 75 (Feb. 2019)
  - Release of report and recommendations (Dec. 2018)
  - Today's presentation

Key Issues

- RPA acceptance/RPA clauses regarding liability
  - Elimination of the RPA vs. possible replacement of indemnification clause with as-is disclaimer
  - Integration of RPA acceptance into validator software
  - Possible creation of new nonprofit for RPKI
- Revisions to the RPA's prohibited conduct clause
- Inclusion of RPKI in procurement requirements
- Information regarding best practices
- Other recommendations

Issue 1: RPA Acceptance/Terms Allocating Liability

- Leading validator software comes preloaded with all Trust Anchor Locators (TALs) except ARIN's
  - Other four RIRs allow TAL access without click-through agreements
  - ARIN requires click-through acceptance of a Relying Party Agreement (RPA)
- Explanations for the difference
  - American law requires actual or constructive knowledge of the agreement
  - Terms need to be in the user's visual field to be clearly binding
- Possible solutions
  - Drop the RPA altogether
  - Keep the RPA, but replace the indemnification clause with an as-is disclaimer

Evaluation of Options

- Drop the RPA
  - Would facilitate the broadest possible distribution of the ARIN TAL
  - Would create uncertainty whether online terms limiting liability are binding
  - Could leave negligence liability in place without being managed by contract
  - Would leave in place risks resulting from the greater litigiousness of U.S.
- Keep the RPA unchanged (ARIN already agreed to consider changes)
- Keep the RPA, but replace the indemnification clause with as-is disclaimer of warranties
  - Comparison with policies of other RIRs and other types of software
  - Simplification of acceptance by inclusion in validator software

Comparison of ARIN with Other RIRs

RIR	Key Clauses Allocating Liability (Paraphrases)
ARIN	• Disclaimers of warranties • Indemnification + duty to defend and hold harmless • Application to actions taken by RP or users downstream of RP
APNIC	• No agreement • Online terms and conditions include indemnification, but no duty to defend or hold harmless
RIPE NCC	• No agreement • Online terms and conditions include disclaimers of warranties
AFRINIC	• No agreement or relevant terms and conditions
LACNIC	• No agreement or relevant terms and conditions

As-Is Disclaimer as an Indemnification Alternative

- As-is disclaimers widely used for other types of software
- Change would block ARIN liability, but create some procedural risks
- There are no direct legal precedents
  - Policy followed by RIPE; no RPKI cases on record
  - No cases on record re TLS, SSL, DNSSec, or IRR
  - Other types of Internet security have more alternatives
  - Note: RSA includes an indemnification clause
  - Caveat: past history does not guarantee future results

A Radical Change: A New Nonprofit for RPKI?

- Another way to manage liability: spin off RPKI certificate repository into an entirely new organization
  - Would be the publisher of the ARIN region RPKI repository (+ others?)
  - Has some precedents: DNS-OARC, PeeringDB
- Potential pros
  - Untethered to existing ARIN operations—might accept more risk
  - Could focus its efforts solely on perfecting RPKI implementation
- Potential cons
  - May run up against history
  - Would require organizational and financial support

Other Ways to Facilitate Risk Management

- Acceptance of RPA is already facilitated by change in ARIN policy permitting integration of RPA acceptance into validator software
- Mechanisms should explore support for acceptance at enterprise level
- RPA can emphasize that any liability does not include consequential damages

- ARIN community should evaluate ways to manage risk

Issue 2: The RPA's Prohibited Conduct Clause

- RPA forbids sharing RPKI info in a "machine-readable format"
  - RIPE prohibits unsanctioned purposes (advertising, market research, etc.)
  - Other RIRs have no analogous provisions
- Clause blocks error reporting and research into performance
  - Machine-readable analysis is crucial
  - ARIN has already agreed to consider permitting non-real time uses
- Clause blocks integration with other info (IRRs, etc.)
- ARIN should consider revisions that allow use of RPKI information as an input into more sophisticated real-time services

Issue 3: Inclusion of RPKI in Procurement Terms

- *Demand* will be a key driver of RPKI adoption more than legal issues
- Customers can incorporate RPKI into procurement specifications
  - Governments
  - ISPs, cloud providers, security services
- Make RPKI something a request companies make of their partners
  - Solves chicken-egg problem by making a collective commitment to security
  - Reflected in ISOC-led Mutually Agreed Norms for Routing Security (MANRS)
    - Includes RPKI as one aspect of filtering (one of four commitments along with anti-spoofing, coordination, and validation)
    - Includes 144 participants

Issue 4: Deployment of Best Practices

- RPKI deployment is only valuable if done safely (esp. failover)
- For network operators, best practices exist
  - Operators should follow the advice of the key RFC 7115 and 6480
  - Operators should solicit advice—from MANRS, Internet2, RIRs
- For RIRs, best practices require disclosure around service levels
  - Includes information on uptime, update frequency, response expectations, etc.
  - Would benefit from expanded Certification Practice Statements
  - Should provide clear guidance about best practices/incentive to deploy them
  - Would benefit from dialogue among RIRs
  - May require greater service commitments by RIRs

Other Issues

- Publicize willingness to waive indemnification/choice of law clauses in the RPA and RSA for government actors legally unable to accept them
- Consider building a non-member services pathway to RPKI as alternative to the Legacy RSA
  - Size of legacy space is shrinking
  - RPKI is still not deploying for IPv6 despite lack of legacy space

Potential Next Steps

- ARIN should consider RPA changes
  - Revising the liability provisions or dropping the RPA
  - Enabling machine-readable redistribution of RPKI info
- The ARIN community should consider whether to support the development of a new nonprofit for RPKI certificate publication
- Network operators and RIRs should focus on best practices and high-leverage tactics like requiring RPKI from vendors
- Everyone interested in enhancing routing security should keep up the momentum

Questions and Discussion